Published on *The National Law Review* https://natlawreview.com

Office for Civil Rights to Increase Investigations of Smaller HIPAA Breaches

Article By:

Rachel Irving Pitts

HHS Office for Civil Rights will cast a wider net and increase its investigations into smaller HIPAA privacy breaches starting this month. OCR announced a new initiative to increase its efforts examining breaches that affect fewer than 500 individuals. OCR Regional Offices already investigate every reported breach affecting 500 or more individuals, and will continue to do so, but now they will intensify efforts to scrutinize smaller breaches.

Investigations into the root cause of even a small breach can discover system- and enterprise-wide noncompliance and security and privacy shortcomings. An investigation into a single stolen laptop that held PHI of 80 individuals may uncover an entity's failure to encrypt any of the data it stores and uses. And just as easily as a larger breach, a small breach can reveal that a covered entity has not completed a full risk assessment of its organization and its PHI protections.

According to OCR,

> Regional Offices will still retain discretion to prioritize which smaller breaches to investigate, but each office will increase its efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these breaches.

Some factors Regional Offices will consider when deciding which breaches investigate include

- theft and improper disposal of unencrypted PHI,
- breaches caused by IT system intrusions like hacking, and
- situations where a covered entity or business associate has numerous reports raising similar issues – indicating a failure to correct systemic problems.

Notably, OCR said Regions can also consider whether a specific entity simply has fewer small

breach reports than similar covered entities and business associates.

OCR highlighted recent settlements from investigations into breaches affecting fewer than 500 individuals. Four of these six settlements involved stolen laptops or other mobile devices with unencrypted data, and another seven-figure settlement resulted from a breach affecting two individuals.

> OCR recognizes that very small breaches can be indicators of very large compliance problems. Accordingly, HIPAA covered entities should never assume that they will avoid scrutiny for reporting a breach affecting fewer than 500 individuals."

This initiative does not change reporting obligations for covered entities – who must still notify the Secretary annually of breaches affecting fewer than 500 individuals. But we can expect OCR's active enforcement of HIPAA breaches to continue unabated, and covered entities and business associates should continue to assess and test their HIPAA compliance proactively, with the goal of avoiding breaches of all sizes.

National Law Review, Volume VI, Number 232